Appl. No. 09/738,248
Amdt. dated January 19, 2005
Reply to Office action of October 20, 2004

REMARKS/ARGUMENTS

Please reconsider the application in view of the above amendments and the following remarks. Applicants thank the Examiner for carefully considering this application.

In the specification, the paragraph [0061] has been amended to correct a minor clerical error.

Claims 1 through 24 remain in this application. Claims 1, 2, 4, 5, 7, 12, 15, 16, 17, 18 and 23 have been amended. Claims 25 and 26 are withdrawn as the result of an earlier restriction requirement. In view of the examiner's earlier restriction requirement, Applicants retain the right to present claims 25 and 26 in a divisional application.

Claim Objections

Claim 7 was rejected because of a minor informality. Applicants have amended claim 7 in accordance with the Examiner's comments.

Claim Rejections

Claims 6, 12, 15-16, and 23 were rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention.

Applicants have amended the above-listed claims to remedy the rejections cited by the Examiner.

Claims 1, 9-17, and 22-24 are rejected under 35 USC 102(e) as being clearly anticipated by Challenger et al "Challenger" (US Patent No.: 6,081,793). Applicants respectfully traverse the Examiner's assertions.

Applicants' present invention discloses a method and system that enables anonymous electronic voting over the Internet using public key technologies. This invention provides for electronic voting over the unsecured network that is the Internet, using the public and private key pair belonging to the voting entity, not a separate user ID and password for each election. In the voting method of the present invention, a voting entity requests a ballot using a public key and a private key belonging to the voting

11

entity. The request is made to a voting mediator. Using a separate public key/private key pair, the voting mediator validates the voting ballot request. After validation of the request, the voting mediator generates an election ballot. The voting mediator sends this ballot to the voting entity. The voting entity casts a vote and sends the ballot to the voting tabulator. The voting tabulator authenticates the ballot and counts the vote. The present invention requires much less communication than the method described in Challenger.

Challenger describes a voting method and system that allows for electronic or paper type ballots to be utilized. In the system, a plurality of cryptographic routines are utilized in a distributed data processing system to maximize the privacy of both the voter's identity and the content of completed ballots. With regard to the assertion in col. 3, lines 10-29, this section merely describes the contents of a smart card used in the implementation of Challenger. This section does not describe the steps involved in implementing the method of Challenger. Any conclusions related to the method of Challenger based on this cite are speculative. Referring to col. 7, line 37 through col. 8, line 53 and Figure 7, Challenger describes its method for electronic voting. Applicants do submit that there are some similarities between the Challenger and Applicants' invention. However, the rationale and implementation of the encryption/decryption steps is distinct.

Applicants' method allows the voting entity to interface directly with the voter mediator. Challenger has several severs involved in the voting process. Applicants' use a public key/private key pair at the voting entity and at the voting mediator. Paragraphs [0058] through [0063] describe the implementing of Applicants' method. The voter initially interacts with the voting mediator to get a ballot. After the voting entity has completed the ballot, the voting entity interacts with the voting tabulator. In both interactions, the voting entity uses its public key/ private key pair to encrypt the voting information.

In Challenger, there is no direct interaction between the voter and the tabular. As shown in Figure 1A of Challenger, several voting severs (authentication, journal and results) are used in the method. These severs interact with each other and the voter in a

12

manner that is different from Applicants' present invention. Referring to the list of the steps for electronic voting in Challenger based on the description from col. 7, line 37 through col. 8, line 53 and Figure 7 of Challenger, uses server public keys to encrypt information. In this method, the journal server interacts with the resulting server to ensure that the information is not tampered with during transmission from the voter to the result server. Applicants' present invention provides a signature by the voting entity using the voting entities private key to prevent decryption and access to the voter information. Although, the Challenger mentions that the voter card has a public and private key, the use of these keys for the electronic voting method of Challenger different is from the use described in Applicants' invention.

For the above stated reasons, Applicants submit that Challenger does not anticipate the present invention.

Claims 2, 5, 7-8, and 21 are rejected under 35 USC 103(a) as being unpatentable over Challenger in view of Kilian et al (US Patent No. 5,495,532). Examiner asserts that Challenger fails to explicitly disclose obtaining a voting certificate from the voting mediator, however, Kilian does disclose a secure voting system which teaches obtaining a voting certificate and authenticating using a key. Kilian describes an algorithm that relies upon a novel mathematical method to encode votes for verification by breaking up the vote into shares, which are supplied to different counting centers. Challenger also appear to incorporate a scheme of dividing up the information as part of the voter security. However, Applicants submit that a combination of Challenger and Kilian would not produce Applicants' present invention. Applicants' approach is to use the public key /private key schemes and not to break up the data. This approach is different from the approach of the cited references. Applicants' submit that the assertion that the present invention is obvious in view of the differences in Applicants' approach is based on an evaluation of Applicants' invention after review of the references. Citing the standard, Graham v. John Deere, "the obviousness standard, while easy to expound, is sometimes difficult to apply. It requires the decision maker to return to the time the invention was made. The invention must be viewed not with the blueprint of drawn by the inventor, but in the state of the art that existed at the time of the invention was ..., that which is clear with the invention fully diagrammed, may have been a breakthrough of substantial

13

dimension when first unveiled.' The courts are clear the it is impermissible to use hindsight to reconstruct the invention from prior art with the invention before the examiner.

Claims 3, 4, 6 and 19-20 are rejected under 35 USC 103(a) as being unpatentable over Challenger in view of Kilian et al and further in view of Witt et al (U.S. Patent No. 6,144,739). The concept of using packaged sealed objects as a security would not be necessary in a combination of Challenger and Kilian. As mentioned, the approach of Challenger and Kilian is to distribute the information and not package it as described in Witt. In addition, Witt does not even discuss or mention applications related to voting. Further, in order to combine references there needs to be some teaching or suggesting of the combination. There is nothing in Challenger or Kilian to suggest a further combining with Witt. The mere existence of a feature in a reference does not mean that the reference in combinable with another reference absent any teaching of the combination. Applicants submit that because of the difference in the approaches between Challenger, Kilian and Witt, there is not motivation to combine these references absent impermissible hindsight.

In view of the above, Applicants respectfully submit that none of the art of record (alone or in combination) teaches, discloses or even suggests the invention as recited in each of Applicant's claims. Applicant further submits that all of the pending claims are in condition for allowance. Withdrawal of the rejections and passage to issuance is respectfully requested. Applicant believes this reply to be fully responsive to all outstanding issues and place this application in condition for allowance. If this belief is incorrect, or other issues arise, do not hesitate to contact the undersigned at the below listed telephone number.

Respectfully Submitted,

Darcell Walker
Reg. No. 34,945
9301 Southwest Freeway, Suite 250
Houston, Texas 77074
713-772-1255
January 19, 2005

14